Spectrum REACH

Brand Safety Guide

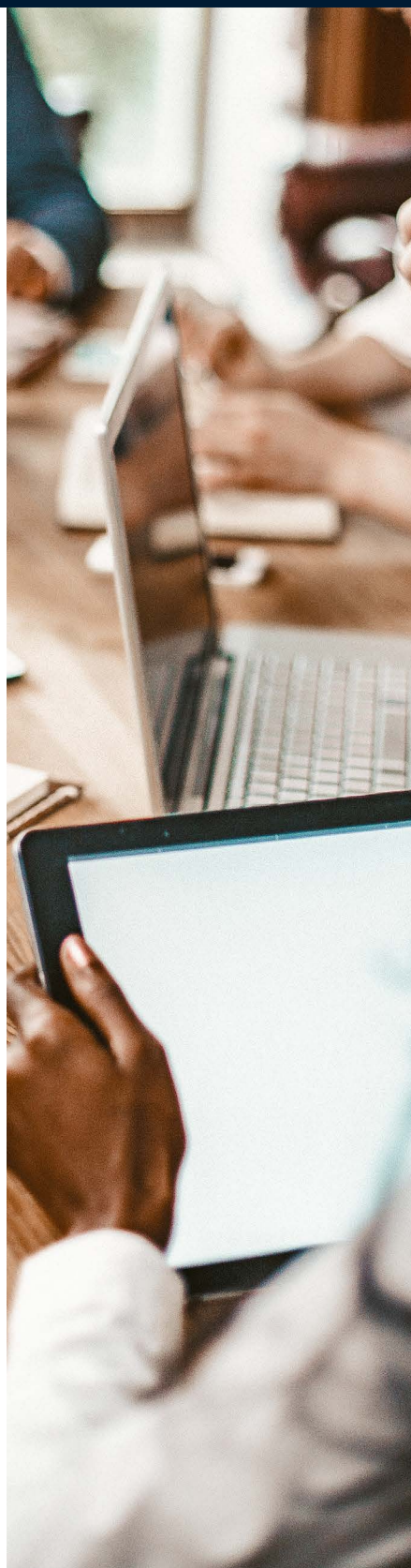
How to Prevent Ad Fraud and Protect Your Ad Spend

On average, in 2020, small and medium-sized businesses lost almost $15,000 annually on ad impressions that were never seen by real people.

Additionally, Digital Agencies experienced average client ad spend losses of $207,000 annually in 2020, over 10 times the amount of SMBs![1]

[1]PPC Global Click Fraud Report 2020-21

How can you prevent ad fraud?



Spectrum Reach, the advertising sales business of Charter Communications, Inc., is at the forefront of the advertising industry initiative to fight criminal activity in the digital advertising supply chain. It is important for advertisers not to rely on publishers when it comes to "grading their own homework," and to demand independent third party verification from trusted MRC accredited partners. Advertisers can better protect themselves and their media investments by independently measuring video completion rates, viewability, and IVT to determine real humans versus bots and real engagements versus lack thereof.

And while an advertiser can do all of this on their own, it is certainly easier and more cost effective to work with an industry leader, like Spectrum Reach, who has the people, processes, knowledge, and partner relationships already in place and set up to protect you from the start. Spectrum Reach adheres to these three practices to ensure you are getting the highest quality, fraud-free streaming TV and online inventory:

1. **Premium Ad Placements:** Spectrum Reach operates a premium pool of inventory consisting of owned and operated properties, in addition to direct deals, carriage agreements, and partner relationships. This ensures no inventory is being aggregated blindly from indirect marketplaces or open exchanges.
2. **Premium Certifications:** Spectrum Reach is a TAG Platinum Status partner, certified against fraud, malware, and piracy, and brand safety certified. These independent certifications are verified by MRC accredited vendors and an external audit to validate that our inventory and acquisition practices are best-in-class.
3. **Premium Verification:** Spectrum Reach partnered with Oracle Moat as our verification partner to validate that all of our inventory has been seen by real people and is held to the highest Key Performance Indicators. We monitor this on a daily basis to ensure ad placements are always delivered on premium content, and provide high performance results.

Understanding Ad Fraud

Ad fraud on streaming TV and online affects almost every advertiser in some way. At a time when many companies are facing budget constraints brought on by economic disruption, you can imagine that now, more than ever before, they want to make sure every dollar counts. By not properly measuring or verifying online or streaming TV inventory, advertisers are putting themselves at significantly higher risk of falling victim to sophisticated schemes and "spoofing" scams designed to generate fraudulent inventory/ad requests that lead to advertisers unknowingly paying for impressions that were never seen. Global digital advertising has grown to $390 billion annually, and cybercriminals want a piece of the action. Juniper Research estimates that the industry loses approximately $51 million per day due to ad fraud and that by 2023 that number will skyrocket to $100 billion annually.

What Does Ad Fraud on Connected TV (CTV) Look Like?

A Connected TV (CTV) is a device that connects to—or is embedded in—a television to support video content streaming. Different types of CTVs include Xbox, PlayStation, Roku, Amazon Fire TV, Apple TV, and more. (Oracle)

In one of the more common types of Ad Fraud on CTV, called 'spoofing,' marketers purchase CTV ads with the promise that their ads will be served to a certain group of people, but the ad impression goes to a different device or a different group of people. Cybercriminals and their bots might mislead marketers that they've paid for more premium advertising than they actually got – or even that there is an ad present when there actually isn't.

What Does Online Ad Fraud Look Like?

Ad fraud is considered an attempt to defraud digital advertising networks for financial gain. Scammers often use bots to carry out online ad fraud, but not always – there are a number of methods including, but not limited to, ad stacking, domain spoofing, and pixel stuffing, that are intended to deceive advertisers and ad networks into paying them.

How Can Advertisers Detect Ad Fraud?

Detecting digital advertising fraud can be difficult. However, there are some warning signs that can help you spot ad fraud, such as:

- High bounce rates for websites
- Reductions in ad spend ROI
- Traffic from unfamiliar sources or non-targeted geolocations
- Abandoned carts
- Sudden large increase in clicks without a proportional increase in conversion

Spectrum REACH®

Types of Ad Fraud Techniques

Bots

Short for robots, hackers create bots to surf the web, click on ads and play videos, which drives up traffic, resulting in more money paid out to the fraudsters. These bots are viruses that can be installed unknowingly on a computer. However, most people with infected computers are completely unaware.

Domain Spoofing

Domain spoofing is a form of fraud where a fraudster impersonates a company's domain in order to pass off low quality inventory as high quality. Fraudsters fool buyers into thinking their ad is going to a premium site, when in reality it's going to a low-quality website. Domain spoofing is also commonly used to mask unsafe sites.

Pixel Stuffing

Serving one or more ads, or an entire ad-supported site, in a single 1×1 pixel frame so ads are invisible to the naked eye.

Ad Stacking

Placing multiple ads on top of each other in a single placement, with only the top ad being viewable. The advertiser is paying for impressions even if the user is not seeing the ads.

Location Fraud

Advertisers pay a premium for their ad to be served in a particular region, but fraudsters will send false location information so the ad actually serves elsewhere.

Cookie Stuffing

Cookies are a method of tracking user behavior to help determine what advertising effort led to a conversion (click, purchase, etc.) or what a user's interests are.

User-Agent Spoofing

The web page "header" that provides a description of the browser is modified to obfuscate information about the browser being used, which can interfere with user targeting. It's most often used by bots trying to hide their tracks.

3 Tips to prevent ad fraud and protect your ad spend.

PICK TRUSTWORTHY PARTNERS

Make sure the partners and publishers you work with have a good reputation in their industry – or, even better, that they are third-party validated for the high standards they have set by the Trustworthy Accountability Group (TAG). TAG Certified Against Fraud status is a designation for companies who have established industry best practices to protect their digital advertising operations from the corroding effects of fraud. TAG Certification differentiates between the companies that are truly committed to fighting cybercrime through high standards, industry collaboration, and threat sharing.

*Spectrum Reach is the **first local media sales organization to achieve TAG Platinum Status** and only the 13th industry leader to achieve **TAG Platinum Status.***

VERIFY, VERIFY, VERIFY!

Use tools to verify ads or use a partner who uses third party verification on your behalf – like Oracle Moat. Do not allow the end vendor to also evaluate their own work. Use industry trusted third parties to audit performance and to help hold your advertising dollars to the highest standard. Investigate when the cost per thousands (CPMs) are too good to be true.

Spectrum Reach is committed to providing advertisers with access to the most diverse and premium pool of ad inventory available, with an emphasis on brand safety and supply standards. In order to deliver on this promise, Spectrum Reach partnered with Oracle Moat Analytics to closely monitor and optimize toward supply quality metrics, such as measurability, viewability, valid traffic, and brand safety. This close attention to detail gives advertisers confidence in the quality of inventory and associated performance metrics, all in a privacy-compliant way.

DEMAND TRANSPARENCY

Quite simply, transparency over your marketing efforts means having oversight over exactly where and how your campaigns are served. Don't trust someone who offers new "ad tech," or who just says that they are high quality or have premium inventory. Demand transparency. Ask to understand how the technology works, what makes their inventory premium, where your ads are running, and who is seeing them.

We put the power in your hands, and give you 24/7 access to our fully-transparent reporting dashboard so you can measure impressions, creative, by device, daypart, and geography, and we offer visibility into video completion rates, and to which websites and networks your message was delivered. Additionally, Spectrum Reach is 100% ads.txt compliant, meaning we utilize a filtered whitelist to ensure ads appear only on quality, brand safe websites and apps that have been vetted and verified as legitimate - so ads are delivered to humans, and not bots, in a fraud-free environment.

Confirming our promise to uphold the highest brand safety standards to protect our clients' advertising on Streaming TV and Online. CONTACT US to experience the Spectrum Reach difference.